

ISO/IEC 11889-1:2009-05 (E)

Information technology — Trusted Platform Module — Part 1: Overview

Table of Contents

1. Scope	1
2. Abbreviated Terms	1
3. The Trusted Platform	4
3.1 Trusted Platform Building Block	4
3.2 The Trust Boundary	4
3.3 Transitive Trust	4
3.3.1 Basic Trusted Platform features	5
3.4 Integrity Measurement	6
3.5 Integrity Reporting	7
4. The TPM	7
4.1 Cryptographic Algorithms Required with TPM	7
4.1.1 Algorithm Assumptions	8
4.2 Operating Systems Supported by TPM	8
4.3 Protected Capabilities	8
4.4 Trusted Platform Module components	8
4.5 Naming Conventions	10
4.6 Privacy Considerations	11
4.7 TPM Operational States	12